

## UNITED STATES DISTRICT COURT

for the  
District of Oregon

## In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*The premises located at 2322 Hillcrest Rd., Medford, OR  
97504, and the person of James HART  
(DOB: XX/XX/1992)

Case No. 1:18-mc- 1038

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:The premises located at 2322 Hillcrest Rd., Medford, OR 97504, and the person of James HART  
(DOB: XX/XX/1992) as described in Attachment A, which is attached and incorporated herein by this reference.located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

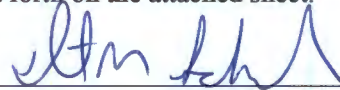
The information and items set forth in Attachment B which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252A(a)(1)	Transportation of visual depictions of minors engaging in sexually explicit conduct
18 U.S.C. § 2252A(a)(2)	Receipt/Distro of visual depictions of minors engaging in sexually explicit conduct
18 U.S.C. § 2252A(a)(5)(B)	Possession of child pornography

The application is based on these facts:  
See affidavit of Special Agent David Schroeder which is attached hereto and incorporated herein by this reference.☒ Continued on the attached sheet.☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.*Applicant's signature*

DAVID M. SCHROEDER, Special Agent, HSI

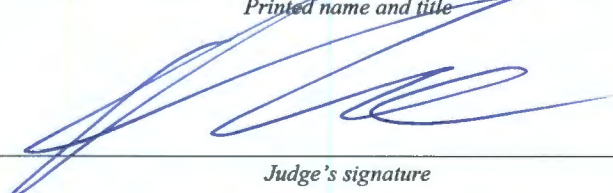
*Printed name and title*

Sworn to before me and signed in my presence.

Date:

11/27/18

City and state: Medford, Oregon

*Judge's signature*

MARK D. CLARKE, U.S. Magistrate Judge

*Printed name and title*

DISTRICT OF OREGON, ss:                   AFFIDAVIT OF DAVID M. SCHROEDER

**Affidavit in Support of an Application  
Under Rule 41 for a Search Warrant**

I, David M. Schroeder, being duly sworn, do hereby depose and state as follows:

**Introduction and Agent Background**

1.       I am a Special Agent (SA) with the United States Department of Homeland Security, Homeland Security Investigations (HSI) in Medford, Oregon. HSI is responsible for enforcing the customs laws, immigration laws, and federal criminal statutes of the United States. I am a law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and I am authorized by law to conduct investigations and to make arrests for felony offenses.

2.       I have been a Special Agent with HSI since September 2010. My duties as a SA include the enforcement of federal criminal statutes prohibiting the sexual exploitation of children, including Title 18, United States Code, Sections 2251 through 2259, the Sexual Exploitation of Children Act (SECA), and Title 18, United States Code, Section 2423(a), which prohibits the interstate transportation of a minor for the purpose of engaging in unlawful sexual conduct. I have been involved in over 50 investigations involving the sexual exploitation of children or the production, distribution, receipt, and possession of child pornography. I have received specialized training in the areas of the importation and distribution of child pornography. I have observed and reviewed numerous examples of child pornography in many forms of media, including video and computer media. I have attended the federal Criminal Investigator Training Program and ICE Special Agent Training at the Federal Law Enforcement Training Center.

3. In addition to my duties as a SA, I have received certifications from the National White Collar Crime Center (NW3C) in Basic Data Recovery and Acquisition (BDRA), Secure Techniques for Onsite Preview (STOP), Intermediate Data Recovery & Analysis (IDRA), Identifying and Seizing Electronic Evidence - Train the Trainer (ISEE-T3), training from the Mentor Forensic Services for the Specialist Interview Course, and training from Cellebrite as a Certified Physical Analyst and Task Instructor.

4. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 2322 Hillcrest Rd., Medford, OR 97504 (hereinafter "Premises"), as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), transportation, receipt, distribution, possession and access with intent to view child pornography. As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located at 2322 Hillcrest Rd., Medford, OR 97504.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

### **Applicable Law**

6. Title 18, United States Code, Section 2252A(a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. Title 18, United States Code, Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term child pornography is defined in Title 18, United States Code, Section 2256(8).

### **Statement of Probable Cause<sup>1</sup>**

---

<sup>1</sup> Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP address.* The Internet Protocol address (or simply “IP address”) is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet.* The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

7. I have been working cybertip investigative leads since 2011. The National Center for Missing and Exploited Children (NCMEC) cybertips are the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. NCMEC then sends the cybertip to the Internet Crimes Against Children (ICAC) task force or other law enforcement agency in the area where the cybertip is located.

8. Since August 2018, I have received six cybertips from the Oregon Department of Justice (OR DOJ) ICAC task force. The six cybertips received at the time of this search warrant are: 31854762, 31855513, 35108014, 36180371, 36232234, and 36234276.

9. Cybertip 31854762 shows Snapchat submitted a tip to the NCMEC which received the tip on 5/5/2018 at 13:47:07 hrs (UTC). Snapchat reported a child exploitation video file named X6PolebySb-SG0-adBAluwAAArT-sHHkS848PAWMvnU68AWMvnT4YAAFRgA was uploaded to Snapchat on 5/5/2018 at 13:47:06 hrs (UTC) from Internet Protocol (IP) address 2003:c0:a71a:2171:b567:5225:cb98:4a2 which geolocated to Germany. The video is 10 seconds in length with sound. The video shows a prepubescent boy lying on his back with

---

c. *Storage medium.* A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

no pants or underwear on with his shirt pulled up to his chest. An adult male is in front of the boy performing oral sex on him and masturbating him. Snapchat provided the following information related to the account:

Phone: 541-840-5004

Date of Birth: 12/17/1992

Approximate Age: 25

Email Address: aaronpierre@hotmail.co.uk

Screen/User Name: hart365

Reported Display Name: James Hart

10. Cybertip 31855513 shows Snapchat submitted a tip to NCMEC which received the tip on 5/5/2018 at 14:00:16 hrs (UTC). Snapchat reported a child exploitation video file named X6PolebySb-SG0-adBAluwAAAaYBH8U0rdhp6AWMvnTqZAWMvnSFtAAFRgA was uploaded to Snapchat on 5/5/2018 at 14:00:16 hrs (UTC) from IP address 2003:c0:a71a:2171:b567:5225:cb98:4a2 which geolocated to Germany. The video is 10 seconds in length with sound. The video shows a prepubescent boy lying on his back with no clothes on and an adult male with some sort of substance on his hand rubbing the boy's genitalia. Snapchat provided the following information related to the account:

Phone: 541-840-5004

Screen/User Name: hart365

11. Cybertip 35108014 shows Instagram submitted a tip to NCMEC which received the tip on 6/21/2018 at 16:03:00 hrs (UTC). Instagram reported three child exploitation image files were uploaded to Instagram on 6/20/2018 between 06:59:58 hrs

(UTC) and 07:00:33 hrs (UTC) from IP address 97.121.54.48.

a. Image

7w4wz0678wcos8o434266238\_596767670701839\_4402914031900295168\_n shows a prepubescent boy lying on a couch on his back, naked. The boy appears to be inserting a cucumber into his anus.

b. Image

8sybb57oehc8osos34601322\_213715402685867\_5372283971604316160\_n shows a minor boy, naked, performing oral sex on a pubescent boy, also naked, on a couch.

c. Image

d7ldrtoayi8sowwg34821008\_2117615041816534\_5122377434015989760\_n shows two prepubescent boys, naked performing oral sex on each other. One boy is lying on top of the other boy with their heads at opposite ends on a bed. Instagram provided the following information related to the account:

Name: Jmh

Screen/User Name: jmh7044

ESP User ID: 7394248794

Phone: 541-840-5004

12. On 8/6/2018, ICAC SA Williamson sent a subpoena to CenturyLink for subscriber information for IP address 97.121.54.48 on 6/20/2018 at 07:00:33 hrs (UTC). CenturyLink responded to the subpoena request and provided the following subscriber information:

Connection Log (GMT): start date 5/25/2018 at 00:58:25 and end date 7/4/2018 at 23:14:03 for IP Address 97.121.54.48.

User: hartlinda238

Phone: 541-772-2629

Subscriber Information: Linda Hart at 2322 Hillcrest Rd, Medford, OR 97504

Length of Service: 5/13/15 to present

13. Cybertip 36180371 shows Microsoft submitted a tip to NCMEC which received the tip on 7/10/2018 at 00:17:27 hrs (UTC). Microsoft reported one child exploitation image file was uploaded to Microsoft OneDrive (cloud-based storage) on 7/9/2018 at 15:04:56 hrs (UTC) from IP address 97.121.15.20. Image d8aefbad-ad5c-4d1f-9cb5-562f367a8cde.jpg is the same image listed in Cybertip 35108014 as image 8sybb57oehc8osos34601322\_213715402685867\_5372283971604316160\_n which shows a minor boy, naked, performing oral sex on a pubescent boy, also naked, on a couch.

Microsoft provided the following information related to the account:

Screen/User Name: 914800525732639

IP Address: 97.121.15.20

14. On 8/10/2018, ICAC SA McBeth sent a subpoena to CenturyLink for subscriber information for IP address 97.121.15.20 on 7/9/2018 at 15:04:56 hrs (UTC). CenturyLink responded to the subpoena request and provided the following subscriber information:

Connection Log (GMT): start date 7/4/2018 at 23:15:48 and end date 7/10/2018 at 09:51:47 for IP Address 97.121.15.20.

User: hartlinda238

Phone: 541-772-2629

Subscriber Information: Linda Hart at 2322 Hillcrest Rd, Medford, OR 97504

15. Cybertip 36232234 shows Microsoft submitted a tip to NCMEC which

received the tip on 7/10/2018 at 14:53:15 hrs (UTC). Microsoft reported one child exploitation image file was uploaded to Microsoft OneDrive on 7/9/2018 at 15:04:53 hrs (UTC) from IP address 97.121.15.20. Image 3c36fd94-8923-4012-986c-9c5d2ff3ad46.jpg shows a prepubescent boy, naked, holding himself on top of an adult male who appears to be inserting his penis into the boy's anus. Microsoft provided the following information related to the account:

Screen/User Name: 914800525732639

IP Address: 97.121.15.20

16. Cybertip 36234276 shows Microsoft submitted a tip to NCMEC which received the tip on 7/10/2018 at 15:20:03 hrs (UTC). Microsoft reported one child exploitation image file was uploaded to Microsoft OneDrive on 7/9/2018 at 15:04:55 hrs (UTC) from IP address 97.121.15.20. Image 06a34836-8008-47cd-8144-6c49ef6d43bf.jpg shows a prepubescent boy lying naked on his back and holding his legs back towards his head. There is an adult male in front of the boy inserting his penis into the boy's anus. Microsoft provided the following information related to the account:

Screen/User Name: 914800525732639

IP Address: 97.121.15.20

17. On 10/19/2018, I sent a summons request to the Sprint Corporation for subscriber information for cellphone number 541-840-5004 which was associated with the Snapchat and Instagram accounts from the first three cybertips. Sprint responded to the summons request and provided the following information related to the account:

Billing Account Number: 304569312

Account Establish Date: 7/8/2012

Account Billing Address Effective 7/8/2012: James Hart of 1679 Rolling Meadows Ln, Medford, OR 97504

Electronic Serial Number: 089595162402187881 effective 11/10/2017

18. I conducted Department of Motor Vehicle (DMV) checks for James HART and found James Morgan HART DOB: XX/XX/1992 with OR driver's license # 2350659 with a listed address of 1679 Rolling Meadows Ln., Medford, OR. DMV checks also showed a 1999 Jeep Grand Cherokee with OR license plate 341FNF registered to HART at 1679 Rolling Meadows Ln, Medford, OR.

19. I conducted computerized criminal history (CCH) checks for HART and found him associated with FBI# 708067JD1 for a 2008 Sodomy in the 1st Degree conviction and a 2017 arrest for failure to register as a sex offender which was later dismissed.

20. On 11/7/2018, I contacted the Oregon State Police (OSP) Sex Offender Registration Unit for current information for HART. OSP reported HART's most recent registered address as 2322 Hillcrest Rd., Medford, OR which is the same address the CenturyLink subpoena returns on the IP addresses used to upload the child exploitation images came back to. OSP also provided a phone number for HART of 541-840-5004 which matches the numbers used to create the Instagram and Snapchat accounts. OSP also provided a mailing address of 1679 Rolling Meadows Ln, Medford, OR which is the same address listed on HART's OR driver's license. The sex offender registration shows the last contact made with HART was on 6/11/2018 at the Hillcrest Rd. address.

21. On 11/14/2018 at approximately 1322 hrs I drove by the residence located at 2322 Hillcrest Rd., Medford, OR. 2322 Hillcrest Rd. appears to be a single-family residence with “2322” in black numbers to the right of the main entrance.

22. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records will likely be found is data stored on a computer’s hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

23. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Based on information received in the Cybertips that Microsoft Bing Image Search was used, it is clear that a computer or digital device was used to view, receive upload, and distribute child pornography. Thus, there is reason to believe that there is a computer, storage medium or digital device currently located on the premises or on the persons containing evidence of the crime.

24. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a

paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring

before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

f. I know that when an individual uses a computer or digital device to commit a crime such as to view, possess, receive and distribute child pornography the individual's computer or digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer or digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer or digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer or digital device used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

25. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for

forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

26. Because several people share the Premises as a residence, it is possible that the Premises will contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the warrant applied for would permit the seizure and review of those items as well.

27. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the

warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

28. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

29. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

30. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

31. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

32. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

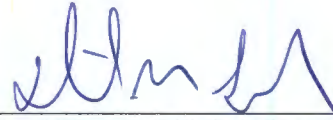
33. The government has made the following prior efforts in other judicial fora to obtain evidence sought under the warrant: subpoenas were issued for user data to identify the location to be searched.

### **Conclusion**

34. Based on the foregoing, I have probable cause to believe, and I do believe, that James HART committed Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), transportation, receipt, distribution, possession and access with intent to view child pornography, and that contraband and evidence, fruits, and instrumentalities of those offense's, as described above and in Attachment B, are presently located at 2322 Hillcrest Rd., Medford, Oregon 97504, which is described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the Premises described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

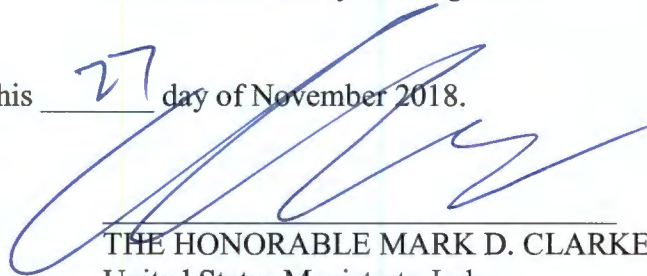
35. Prior to being submitted to the Court, this affidavit, the accompanying

application, and the requested search warrant were all reviewed by Assistant United States Attorney Judi Harper, and AUSA Harper advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.



DAVID M. SCHROEDER  
Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me this 27 day of November 2018.



THE HONORABLE MARK D. CLARKE  
United States Magistrate Judge

**ATTACHMENT A**

**DESCRIPTION OF PREMISES TO BE SEARCHED**

1. The premises, including the dwelling, shed, and curtilage is located at 2322 Hillcrest Rd., Medford, Oregon 97504, further described as a greenish-gray in color house. 2322's main entrance is setback and faces west. The residence faces north towards Hillcrest Rd. To the left of the garage door is "2322" in black numbers identifying the residence. The premises to be searched include all rooms, attics, garages, sheds, or storage rooms, whether attached or detached.



## **ATTACHMENT B**

### **Items to Be Seized**

The items to be searched for, seized, and examined, are those items on the premises located at at 2322 Hillcrest Rd., Medford, Oregon 97504, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), transportation, receipt, distribution, possession and access with intent to view child pornography. The items to be seized cover the period of May 5, 2018 through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

b. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

e. Any and all records, documents, or materials relating to the production, reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, and e-mail messages.

h. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, receiving, or transporting child pornography, including chat logs, call logs, address book or contact list entries, and digital images sent or received.

i. Computers, storage media, or digital devices used as a means to commit the violations described above, including accessing and viewing child pornography.

j. All content related to the six Cybertips that may further the investigation: 31854762, 31855513, 35108014, 36180371, 36232234, and 36234276.

2. As used in this attachment, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter “Computer”):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer,

such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

- c. Evidence of the lack of such malicious software.
- d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.
- e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.
- f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.
- h. Evidence of the times the Computer was used.
- i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.
- j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.
- k. Records of or information about Internet Protocol addresses used by the Computer.
- l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records

of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

### **Search Procedure**

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to

examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.